Addendum to "Quantum secret sharing between multiparty and multiparty without entanglement"

Fu-Guo Deng,[1,2,] Feng-Li Yan,[3,4] Xi-Han Li,[1] Chun-Yan Li,[1] Hong-Yu Zhou[1,2] and Ting Gao [4,5]

[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education,*
and Institute of Low Energy Nuclear Physics,
Beijing Normal University, Beijing 100875, China
[2] *Beijing Radiation Center, Beijing 100875, China*
[3] *College of Physics Science and Information Engineering,*
Hebei Normal University, Shijiazhuang 050016, China
[4] *CCAST (World Laboratory),*
P.O. Box 8730, Beijing 100080, China
[5] *College of Mathematics and Information Science,*
Hebei Normal University, Shijiazhuang 050016, China

(Dated: February 1, 2008)

Recently, Yan and Gao proposed a quantum secret sharing protocol between multiparty (m members in group 1) and multiparty (n members in group 2) using a sequence of single photons (Phys. Rev. A **72**, 012304 (2005)). We find that it is secure if the quantum signal transmitted is only a single photon but insecure with a multi-photon signal as some agents can get the information about the others' message if they attack the communication with a Trojan horse. However, security against this attack can be attained with a simple modification.

PACS numbers: 03.67.Dd, 03.67.Hk, 89.70.+c

In general, secret sharing [1] is used to split a message (M_A) into several pieces which are distributed to several agents. When the agents collaborate, they can obtain the message, otherwise they can get nothing. Quantum secret sharing (QSS) is the generalization of classical secret sharing into quantum scenario and becomes an important branch of quantum communication. It provides a secure way for not only creating a private key among several users [2, 3, 4, 5, 6, 7] but also splitting a piece of classical secret message or quantum information (an unknown quantum state) [10, 11, 12, 13, 14, 15, 16, 17, 18]. It has progressed quickly since Hillery, Bužek and Berthiaume [2] proposed the original QSS protocol using a three-photon entangled Greenberger-Horne-Zeilinger states, and attracts a lot of attentions in recent years [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21].

Recently, Yan and Gao [19] presented a novel concept for quantum secret sharing of classical information (a private key), i.e., QSS between group 1 and group 2 with polarized single photons. It is secure if the quantum signal transmitted is only a single photon but insecure with a multi-photon signal as some agents can get the information about the others' message if they attack the communication with a Trojan horse. In this paper, we will discuss this attack and improve the security of Yan-Gao QSS protocol against this attack with a little of modification.

The basic idea of Yan-Gao QSS protocol [19] can be described as follows. The members of group 1 are Alice 1, Alice 2,..., and Alice m, and those for group 2 are Bob 1, Bob 2, ..., and Bob n. Group 1 wants to share a private key with group 2 in such a way that the key can be read out only when all members in each group cooperate. This task can be completed with six steps as follows.

(1) Alice 1 generates two random binary strings A_1 and B_1 whose length is nN bits. She also prepares nN qubits and divides it into to n pieces. Each piece contains N qubits. Each qubit is in one of the four states

$$|\psi_{00}\rangle = |0\rangle, \tag{1}$$
$$|\psi_{10}\rangle = |1\rangle, \tag{2}$$
$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3}$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{4}$$

where $|0\rangle$ and $|1\rangle$ are the two eigenvectors of the operator σ_z (called it the measuring basis (MB) Z), and $|+\rangle$ and $|-\rangle$ are those of the operator σ_x. That is, Alice 1 prepares the qubits according to the bit values in A_1 and B_1. The four states $|0\rangle, |1\rangle, |+\rangle$, and $|-\rangle$ correspond to the codes 00, 10, 01, and 11, respectively. The first bit in each code comes from the A_1 and represents the information of the eigenvalue correlated to the state, and the second bit comes from the B_1 and represents the MB of the state, i.e., the state is the eigenvector of Z if the second bit is 0, otherwise the state is the eigenvector of X. Alice 1 sends the nN qubits to Alice 2.

(2) Similar to Alice 1, Alice 2 creates two random binary strings A_2 and B_2. She operates each of the nN qubits according to the bits in the two strings in turn, i.e., if the bit in A_2 is 0, she performs the unitary operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ on the qubit, otherwise she performs the unitary operation $U = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$. Simultaneously she has to operate the qubit according

to the bit in B_2. That is, if the bit in B_2 is 0, she supplies the unitary operation I on the qubit, otherwise she performs a Hadamard (H) operator on it. After the two operations on each qubit, Alice 2 sends the nN qubits to Alice 3.

The nice feature of the operation U is that it flips the state in both measuring bases [4, 22, 23], i.e.,

$$U|0\rangle = -|1\rangle, \qquad U|1\rangle = |0\rangle, \qquad (5)$$
$$U|+\rangle = |-\rangle, \qquad U|-\rangle = -|+\rangle. \qquad (6)$$

The H operation can transfer the states between the two MBs, Z and X [12, 13], i.e.,

$$H|0\rangle = |+\rangle, \qquad H|1\rangle = |-\rangle, \qquad (7)$$
$$H|+\rangle = |0\rangle, \qquad H|-\rangle = |1\rangle. \qquad (8)$$

After the two operations done by Alice 2, the photon is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, which will prevent Alice 1 from eavesdropping freely if there is one photon in each signal.

(3) Alice i operates the qubits like Alice 2, $i = 3, 4, \ldots, m$.

(4) Alice m sends N qubits to each member of group 2, Bob j ($j = 1, 2, \ldots, n$) in turn. After they receive the qubits, the members of group 1 publicly announce the strings $B_1, B_2, \ldots,$ and B_m, which will reveal the information about the MB of each qubit operated by Alice i ($i = 1, 2, \ldots, m$).

(5) Bob j measures each of his qubits with MB Z or X according to the XOR (i.e., $\oplus$) results of corresponding bits in the strings $B_1, B_2, \ldots,$ and B_m.

(6) All members in group 1 check eavesdropping of this quantum communication. If the channel is secure, the XOR results of Bob j's corresponding bits can be used as key bits for secret sharing.

Yan-Gao protocol may be secure for each member in group 2, say Bob j, as group 1 can detect the eavesdropping done by them, as the same as BB84 quantum key distribution protocol [24]. But the eavesdropping done by some members in group 1 is difficult to be detected, in particular some agents in group 1 eavesdrop the communication with a multi-photon signal. We will discuss the security of Yan-Gao protocol and present a possible improvement of Yan-Gao protocol security.

The attack done by Alice 1 with a Trojan horse works as follows. She prepares two photons in the same state and sends them to Alice 2. After operations have been done by the other members in group 1, Alice 1 intercepts the signal and separates a photon from the signal with a photon number splitter (PNS: 50/50). She sends the other one in each signal to the members in group 2. After Alice i ($i = 1, 2, \ldots, m$) announces the strings $B_1, B_2, \ldots,$ and B_m, Alice 1 can obtain the key freely without the help of the others in group 1. It means that Yan-Gao protocol is not secure for Alice 1. Of course, an eavesdropper, Eve (who can be any one of Alice 2, Alice 3, ..., Alice m) can steal almost all the information about the unitary operation done by any member in group 1

with a multi-photon Trojan horse attack except for Alice 1, as the same as that in Ref. [13]. That is, Eve intercepts the original signal and sends Alice i 2^{K+1} photons in the same state, say $\phi_0 = |0\rangle$. After the operation is done by Alice i, Eve intercepts the photons and measures with two MBs after splitting it using some PNSs. In detail, Eve measures half of the photons with MB Z, and the others with MB X. The effect of the two operations $\{I, U\}$ according to A_i and $\{I, H\}$ corresponding to B_i done by Alice i is equivalent to one of the four operations $\{I, U, H, \bar{H}\}$ chosen according to the two bits from A_i and B_i. Here $\bar{H} = \frac{1}{\sqrt{2}}(-|0\rangle\langle0| + |0\rangle\langle1| + |1\rangle\langle0| + |1\rangle\langle1|)$. The task of the eavesdropping done by Eve is simplified to distinguish the four unitary operations. However, they can be distinguished with sufficiently enough photons. If Alice i performs one of the two operations $\{I, U\}$ on the fake signal, the outcomes of the measurements on the 2^K photons with MB Z are the same one, otherwise the outcomes are different. The same result can be obtained with the measurements on the other 2^K photons with MB X if Alice i performs one of the two operations $\{H, \bar{H}\}$ on the fake signal. Thus, quantum secret sharing between m members and n members turns into that between t members ($t < m$) and n members. However, since Alice 1 keep A_1 in secret and Eve can not get the information A_1 of Alice 1, so two groups still share a secure key. In a word, Yan-Gao protocol is not secure only if Alice 1 replaces the single-photon signal with a multi-photon one.

In essence, the attack comes from the two facts: one is that the member in group 1 does not determine whether there is one photon in each quantum signal received or more; the other is that the member does not know whether an eavesdropper intercepts the original signal.

For improving the security of Yan-Gao protocol [19], a photon number splitter (PNS: 50/50) and single-photon measurements are necessary for each of the members in group 1, as the same as that in Ref. [13], except for Alice 1, the one who prepares the original signal. The measurements with a PNS is shown in Fig.1. That is, Alice l chooses randomly a sufficiently enough subset of the nN photons as the samples for eavesdropping check, and measures each sample with a PNS and two single-photon detectors after the original quantum signals are transmitted from Alice $l - 1$ to her, see Fig.1.

For the integrity, let us describe all the steps of this modified Yan-Gao protocol as follows, including some steps same as those in the original one [19].

(M1) Same as the first step in the original Yan-Gao protocol, Alice 1 prepares nN qubits and each qubit is in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ according to the bits in the two binary strings A_1 and B_1. She sends the qubits to Alice 2.

(M2) Similar to Alice 1, Alice 2 create two binary strings A_2 and B_2. For each of the nN qubits, she performs the operation I (U) on it if the corresponding bit in A_1 is 0 (1). Simultaneously she has to operate the qubit with I or H according to the corresponding bit in
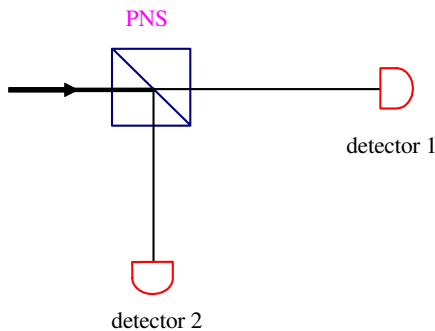
FIG. 1: (Color online) The measurements with a photon number splitter (PNS: 50/50), similar to that in Ref. [13]. The members in group 1 choose one of the two MBs, Z and X, randomly to measure each signal after the PNS.

B_2 is 0 or 1, respectively. She sends the photons to Alice 3.

Certainly, before Alice 2 operates the nN photons, she chooses randomly a sufficiently enough subset of photons as the samples for eavesdropping check. First, she splits each sample signal with a PNS, and then measures each signal with the MB Z or X choosing randomly, shown in Fig.1. Moreover, she should analyze the error rate ε_s of the samples by means that she requires Alice 1 to tell her the original states of the samples. If the error rate is reasonably lower than the threshold ε_t, Alice 2 continues the quantum communication to next step, otherwise she aborts it.

(M3) Alice i operates the qubits like Alice 2, $i = 3, 4, \ldots, m$. For analyzing the error rate of the samples, she requires all the members before her to tell her the

original state or the operations they chose.

(M4) Alice m sends N qubits to each member in group 2, Bob j $(j = 1, 2, \ldots, n)$ in turn. After they receive their qubits, the members in group 1 publicly announce the strings $B_1, B_2, \ldots, B_m$.

(M5) Bob j measures each of his qubits with the MB Z or X according to the XOR (i.e., $\oplus$) results of corresponding bits in the strings $B_1, B_2, \ldots, B_m$.

(M6) All members in group 1 complete the error rate analysis of the transmission between the two groups. To this end, all Alice require each of the member in group 2 to publish a subset of results chosen randomly, and analyze the error rates of the samples. If the channel is secure, the XOR results of Bob j's corresponding bits can be used as key bits for secret sharing, otherwise they discard the results obtained and repeat the quantum communication from the beginning.

In fact, this modified Yan-Gao protocol is secure with just a little of modification of the original Yan-Gao protocol [19]. That is, each of the members in group 1 performs an eavesdropping check for the transmission of the qubits with a PNS and two single-photon detectors. The principle of the eavesdropping checks is the same as that in BB84 quantum key distribution protocol [24, 25]. So the transmission of qubits between two authorized members in the two groups is secure.

[1] G. R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp.313-317; A. Shamir, Commun. ACM **22**, 612 (1979).

[2] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829(1999).

[3] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[4] F. G. Deng, H. Y. Zhou, and G. L. Long, Phys. Lett. A **337**, 329 (2005).

[5] F. G. Deng, G. L. Long, and H. Y. Zhou, Phys. Lett. A **340**, 43 (2005); F. G. Deng et al., Chin. Phys. Lett. **21**, 2097 (2004).

[6] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).

[7] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).

[8] Z. J. Zhang, Phys. Lett. A **342**, 60 (2005).

[9] Z. J. Zhang and Z. X. Man, Phys. Rev. A **72**, 022303 (2005).

[10] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).

[11] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad,

Phys. Rev. A **65**, 042320 (2002).

[12] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Rev. A **71**, 044301 (2005).

[13] F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, Phys. Rev. A (in press), e-print quant-ph/0506194.

[14] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[15] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A **324**, 420 (2004).

[16] F. G. Deng, C. Y. Li, Y. S. Li, H. Y. Zhou, and Y. Wang, Phys. Rev. A (in press); e-print quant-ph/0501129.

[17] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou and H. Y. Zhou, Phys. Rev. A (in press); e-print quant-ph/0504158.

[18] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[19] F. L. Yan and T. Gao, Phys. Rev. A **72**, 012304 (2005).

[20] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[21] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004); A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam, Phys. Rev. A **71**, 033814 (2005).

[22] F. G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004).

[23] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004); e-print quant-ph/0408102.

[24] C. H. Bennett and G. Brassard, *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore,* India (IEEE, New York, 1984), pp.175-179.

[25] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999); P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).